DOI 10.37882/2223-2966.2024.05.18

К ВОПРОСУ ОБ АВТОМАТИЗАЦИИ ПРОЦЕССА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НЕФТЕСЕРВИСНЫХ ПРЕДПРИЯТИЙ: ПОТЕНЦИАЛ, ОБЛАСТИ ПРИМЕНЕНИЯ

ON THE ISSUE OF AUTOMATING THE PROCESS OF ENSURING INFORMATION SECURITY OF OILFIELD SERVICE ENTERPRISES. POTENTIAL, AREAS OF APPLICATION

A. Krasnov
K. Lystsev
I. Chekanov

Summary. Information security in modern society is of paramount importance. To study the areas of potential automation of information security processes oilfield service enterprises are chosen, because their activities contain all the key elements of modern commercial production companies. In the process of the research the key elements of information security of oilfield service enterprises, as well as the features and tasks of the local information security system are separately identified. In addition, the specifics of establishing the regime of trade secrets, and, as a consequence, the organization of work on its protection are outlined.

Keywords: oilfield service enterprises, management, automation, information system, protection.

Краснов Андрей Евгеньевич
Доктор физико-математических наук, профессор, Федеральное государственное бюджетное образовательное учреждение высшего образования Российский государственный социальный университет
krasnovmgutu@yandex.net
Лысцев Константин Сергеевич
Аспирант, Федеральное государственное бюджетное образовательное учреждение высшего образования Российский государственный социальный университет
Konstantin.Lystsev@bk.ru
Чеканов Иван Романович
Аспирант, Федеральное государственное бюджетное образовательное учреждение высшего образования Российский государственный социальный университет
cartmen98@yandex.ru

Аннотация. Информационная безопасность в современном обществе приобретает первостепенное значение. Для изучения областей потенциальной автоматизации процессов обеспечения информационной безопасности выбраны нефтесервсные предприятия, поскольку их деятельность содержит все ключевые элементы современных коммерческих производственных компаний. В процессе исследования отдельно выделены ключевые элементы информационной безопасности нефтесервисных предприятий, а также особенности и задачи локальной системы информационной безопасности. Кроме того, обозначена специфика установление режима коммерческой тайны, и, как следствие, организации работы по ее защите.

Ключевые слова: нефтесервисные предприятия, управление, информационная безопасность, автоматизация, защита.

Введение

Нефть и природный газ являются основными отраслями энергетического рынка и играют влиятельную роль в мировой экономике в качестве основных источников топлива. Процессы и системы, связанные с добычей и распределением нефти и газа, очень сложны, капиталоемки и требуют самых современных технологий [1]. В тоже время, играя жизненно важную роль в мировой экономике, нефтегазовая отрасль является главной мишенью для киберугроз. В ее работе задействованы такие важные объекты инфраструктуры, как нефтеперерабатывающие заводы, трубопроводы и буровые установки. В условиях растущей цифровизации и взаимосвязанности систем обеспечение надежных мер информационной безопасности имеет огромное значение. Чтобы обеспечить защиту от информационных атак в нефтегазовой отрасли, необходимо применять комплексный междисциплинарный подход, который к тому же должен быть синхронизирован. Это способствует гармоничной интеграции бизнес-операций и технологических достижений.

Важным фактором необходимости построения эффективной системы информационной безопасности нефтесервисных предприятий является их последовательная интеграция в информационные системы вертикально-интегрированных нефтяных и газовых компаний. Осуществляя свою деятельность на объектах таких компаний, нефтесервисные предприятия включаются в их информационное пространство, для работы в специально создаваемых информационных системах. На сегодняшний день такие системы реализованы в сегментах оформления пропусков для проезда на лицензионные участки (месторождения), производственные объекты, аккредитации субподрядных организаций, базы дан-

ных обученности персонала, обмена производственным сводками. Все вертикально-интегрированные нефтяные и газовые компании являются субъектами критической информационной инфраструктуры, имеют значимые категории, в связи с чем, включение требований по уровню информационной безопасности в нефтесервисных предприятиях в состав квалификационных показателей на стадии проведения тендеров вопрос времени и является неизбежным.

Таким образом, принимая во внимание тот факт, что последствия успешных атак на информационные системы нефтесервисных предприятий могут быть серьезными и привести к физическому ущербу, перебоям в производстве, экологическим катастрофам и значительным финансовым потерям, вопросы, связанные с обеспечением их информационной безопасности, являются актуальными, что и обуславливает выбор темы данной статьи.

Ключевые элементы информационной безопасности нефтесервисных предприятий

По мере того, как все операционные системы нефтесервисных компаний переходят в режим онлайн и беспрепятственно соединяются с Интернетом вещей (IoT), их уязвимость и подверженность кибератакам возрастают в геометрической прогрессии. Цифровизация должна осуществляться одновременно с созданием надежной системы информационной безопасности [2].

Реагирование на кибератаки должно быть многоуровневым, отражающим наиболее распространенные угрозы и имеющим адаптивный подход к современным и новым векторам уязвимостей и рисков. В тоже время, система должна быть достаточно гибкой, чтобы воспринимать и адаптироваться к сложностям, возникающим в любой момент в результате интеграции IoT, и при этом придерживаться протоколов, регулирующих такие технологические инструменты, как роботизированная автоматизация процессов, блокчейн и искусственный интеллект.

В настоящее время, свойства и характеристики процесса организации информационной безопасности предприятия подробно описаны и стандартизированы, установлены универсальные методы и средства, используя которые предприятие обеспечивает свою защищённость и информационную безопасность. Несмотря на универсальность подходов по организации информационной безопасности, надежность такой системы, в значительной мере зависит от правильного определения рисков, присущих конкретному предприятию. [3].

Особенностью условий труда в нефтесервисных предприятиях являются непрерывный характер, высокая степень механизации, автоматизация. Местом проведения работ являются обособленно обустроенная местность — месторождения, расположенные, как правило, на большом удалении от населённых пунктов. Перечисленные факторы, приводят к тому, что предприятия применяют вахтовый метод работы, содержат большой штат персонала.

Внутренние локальные документы нефтяных компаний, требования федерального законодательства устанавливают высокие требования к обучению персонала, состоянию здоровья, периодичности медицинских обследований.

Федеральный Закон «О защите персональных данных» с момента принятия, до сегодняшнего времени претерпел 29 дополнений и изменений, что свидетельствует об особой актуальности регулируемых им вопросов, и постоянной адаптации его требований к меняющимся реалиям [4]. Наиболее значимыми дальнейшими изменениями являются инициативы по повышению ответственности за утечку персональных данных. В настоящее время в России закончили работу над законопроектом об оборотных штрафах за утечки персональных данных. Итоговая версия предусматривает наказание за подобные инциденты до 3 % совокупной выручки компаний [5].

Нефтесервисный рынок отличается высокой степенью конкуренции, в связи с чем в сегменте информационной безопасности возникает необходимость защиты коммерческой информации. Конкурирующие компании по-разному подходят к организации производства, использованию финансовых инструментов, оптимизации затрат. Данная информация является критической для компании и подлежит защите.

Несмотря на то, что в законе зафиксированы вполне понятные и достаточно простые формулировки и определения, поддежка режима коммерческой тайны, и, как следствие, организация работы по ее защите требует большого объёма действий и мероприятий.

Для введения такого режима использования информации требуется глубокий аудит оборота информации, определение наиболее значимой и критической, требующей защиты. Требуется аудит сотрудников, допущенных к работе с такой информации, принятие административных мер, в виде подготовки регламентов, распоряжений, приказов, дополнений к трудовым договорам, технические меры контроля.

Нефтесервисные предприятия относятся к действию ФЗ № 187 «О критической информационной инфраструктуре» [6]. Это еще одно направление деятельности в области информационной безопасности. Данное направ-

ление требует постоянного взаимодействия с органами государственной власти, такими как Федеральная Служба Технического и Экспортного Контроля (ФСТЭК), Национальный Центр Компьютерных Инцидентов (НЦКИ).

Согласно п. 6 ст. 2 ФЗ № 187 «О критической информационной инфраструктуре», критическая информационная инфраструктура (КИИ) — объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов.

Область и потенциал автоматизации системы информационной безопасности нефтесервисных предприятий

Приведенная информация наглядно демонстрирует важность информационной безопасности для функционирования предприятия, в связи с чем возникает потребность в систематизации, накоплении, сохранении сведений, постоянное улучшение процессов. Поскольку, относительно основных бизнес-процессов, информационная безопасность является вспомогательной функцией, ее организация и поддержание должны осуществляется последовательно, затраты не должны быть избыточными, с одной стороны обеспечивающими необходимый уровень защиты, с другой стороны, не отвлекающими избыточные затраты от основных бизнес-процессов.

Основные проблемы информационной безопасности на нефтесервисных предприятиях включают в себя следующее.

Сложные киберугрозы — их источником могут быть государственные структуры и преступные синдикаты. Отрасль сталкивается со сложными современными постоянными угрозами (APT), вследствие чего злоумышленники стремятся получить несанкционированный доступ к ценной интеллектуальной собственности, такой, например, как технологии бурения, данные о пластах или стратегические планы.

Уязвимости промышленных систем управления (ICS) — системы операционных технологий (OT), включая распределенные системы управления (DCS) и системы диспетчерского контроля и сбора данных (SCADA), подвержены информационным атакам. Это особенно актуально для последних, учитывая их длительный срок службы и отсутствие мер безопасности. Такие устаревшие системы часто не имеют регулярных обновлений безопасности (если таковые имеются) и надлежащей сегментации; ограниченные средства контроля безопасности делают их уязвимыми для эксплуатации. Кроме того, многие из них нелегко исправить или обновить, что делает их восприимчивыми к известным уязвимостям.

Инсайдерские угрозы — несанкционированный физический доступ к критической инфраструктуре может привести к взлому или разрушению систем. Другие так называемые внутренние угрозы представляют собой серьезную проблему, поскольку недовольные сотрудники, подрядчики или другие лица, получившие предварительный авторизованный доступ, могут намеренно или непреднамеренно скомпрометировать критически важные системы и данные.

Удаленные операции — растущая зависимость отрасли от удаленных операций и устройств IoT создает новые проблемы безопасности. Использование технологий удаленного доступа и взаимосвязь устройств увеличивают поверхность атаки, поэтому для снижения рисков требуются строгие меры безопасности.

Риски цепочки поставок — взаимосвязанный характер нефтесервисных предприятий приводит к появлению слабых мест в работе с третьими сторонами — поставщиками и продавцами. Лица, имеющие привилегированный доступ, могут использовать уязвимости, скомпрометировать системы или непреднамеренно раскрыть критическую информацию. Кроме того, нарушенная цепочка поставок может привести к внедрению вредоносного программного обеспечения или аппаратных компонентов.

Кроме того, необходимо отметить, что на сегодняшний день система информационной безопасности, зачастую, носит фрагментарный характер, для ее функционирования используются разные системы хранения данных, что несет риски утраты информации. В этой связи, логичным решением является локальная система информационной безопасности, развернутая непосредственно на сетевых ресурсах предприятия, функционирующая на принципах аутентификации пользователей и разграничении уровней доступа и прав.

Такая система может решать следующие задачи информационной безопасности:

- накопление и сохранность информации, что снижает риск ее утери, или удаления в случае ротации персонала;
- поддержание внутренних нормативных документов в актуальном состоянии, при истечении планового срока обновления, изменения законодательства, внедрения новых технических решений основного производства;
- организация процесса обучения и тестирования персонала по вопросам информационной безопасности с отражением и сохранением результатов, повторное обучение и тестирование при истечении планового срока, перевода сотрудников на другую или вышестоящую работу.

Последние два функциональных решения имеют большой потенциал для интеграции с другими внутренними системами, используемыми в Компании, например, с различными модулями 1С, такими как ЗУП, ERP, а также внешними информационными ресурсами, осуществляющими мониторинг законодательных изменений, такими как «Гарант», «Консультант плюс».

Как указывалось, выше, нефтесервисные предприятия являются объектами критической информационной инфраструктуры. Соблюдение требований ФЗ № 187 требует постоянного документооборота, начиная от первичного категорирования, до регулярного категорирования вновь вводимых объектов основных средств, исключения выбывающего оборудования. Составление и реализация планов и моделей угроз и т.д. Данный процесс имеет значительный потенциал для автоматизации и ее реализации внутри рассматриваемой локальной информационной системы.

В части подготовки документов по категорированию, выбытию объектов критической информационной инфраструктуры автоматизация могла бы быть реализована за счет загрузки в систему шаблонов документов, и создание информационного блока с накоплением информации относительно предприятия, должностных лиц, объектов критической информационной инфраструктуры и их технических характеристик. Техническое формирование документов могло бы быть реализовано за счет миграции данных из информационного блока в шаблоны, с получением готового документа, который, после проверки специалистом, может быть использован предприятием.

Описанный функционал, может быть реализован на базе автоматизированной системы поддержки принятия управленческих решений в области ИБ (АСППУРИБ), с использованием технологии экспертных систем [7].

Заключение

Подводя итоги, отметим, что в современных условиях перед нефтесервисными предприятиями стоит задача по обеспечению информационной безопасности. Это обусловлено, с одной стороны, спецификой организации труда и производственных процессов, а, с другой, — требованиями законодательства Российской Федерации.

Обеспечение информационной безопасности достигается совокупностью технических и организационных мер.

Основные элементы информационной безопасности, такие как защита персональных данных, коммерческой информации, критической информационной инфраструктуры являются объектами государственного регулирования, что требует постоянного анализа принимающих предприятием мер на достаточность и актуальность.

Перспективным направлением деятельности, является автоматизация ряда направлений информационной безопасности путем создания и использования локальной информационной системы.

Данная система способна обеспечить накопление и сохранность информации, обеспечить доступ к ней только авторизированных пользователей, снизить трудозатраты и повысить эффективность подразделений информационной безопасности, за счет автоматизации подготовки распорядительных документов, в первую очередь по вопросам категорированию и защиты критической информационной инфраструктуры, поддержание их в актуальном состоянии.

Реализация такой системы позволит оптимизировать затраты предприятия на обеспечение информационной безопасности, повысить конкурентное преимущество за счет непрерывных улучшений и соответствия бизнес-процессов требованиям законодательства Российской Федерации.

ЛИТЕРАТУРА

1. Интернет издание «Нефтегаз.RU». «Роль и назначение нефтегазового сервиса». https://neftegaz.ru/analisis/oil_gas/329673-rol-i-naznachenie-neftegazovogo-servisa/?ysclid=lo4cqtilfq226323446
2. Родичев Ю.А. «Информационная безопансоть. Национальные стандарты Российской Федерации». Издательство «Питер» СПБ. 2023 г
3. Лысцев К.С. «Принципы построения системы информационной безопасности нефтесервисных предприятий в современных условиях». Сборник материалов 14 международной научно-практической конференции «Развитие науки и практики в глобально меняющемся мире в условиях рисков». Москва, 15 февраля 2023 года Махачкала. Издательство «АЛЕФ» стр. 120–124.
4. Информационный сервис «Консультант плюс» https://www.consultant.ru/document/cons_doc_LAW_61801/.
5. Информационный портал «РБК». https://www.rbc.ru/technology_and_media/27/07/2023/64c15e069a79474102dac8b0?ysclid=lpcg7r0xzb873075781&from=copy.
6. Информационный сервис «Консультант плюс» https://www.consultant.ru/document/cons_doc_LAW_48699/
7. Краснов, А.Е. Автоматизация поддержки принятия управленческих решений в области информационной безопасности на основе технологии экспертных систем / А.Е. Краснов, И.Р. Чеканов, И.Д. Козочкин // Информатизация образования и науки. — 2023. — № 2(58). — С. 81–89. — EDN TKLBEM.

© Краснов Андрей Евгеньевич (krasnovmgutu@yandex.net); Лысцев Константин Сергеевич (Konstantin.Lystsev@bk.ru);
Чеканов Иван Романович (cartmen98@yandex.ru)
Журнал «Современная наука: актуальные проблемы теории и практики»